I2DS24 exercise 3

Wolfgang J. Paul

March 10, 2024

1 Leader Election in Rings (20 Pt)

This proceeds in rounds $r \geq 1$. Messages in round r have the format (m, r), i.e. they contain the round number. In each round r as set $S(r)$ of surviving candidates is left. These sets will shrink very quickly.

Initially $S(1) = [0 : n - 1]$ is the set of all processes. Round r :

- each surviving process $i \in S(r)$ produces a random number $R_i = \text{random}(N)$ and sends (R_i, r) to the right. Then the round is completed as in the LCR algorithm, but processes count steps.
- If all random numbers chosen are different, then the node i with the largest R_i declares itself the leader, when it receives its own number after N steps.
- every node which does not receive its own number within N step leaves $S(r+1)$.
- every node which receives its own number within less than N steps remains in $S(r+1)$.

```
S(1) ← [0 : N − 1]                    ▷ Initially S(1) is the set of all processes
r ← 1
while true do
    for all i ∈ S(r) do
        R_i ← random(N)
        uid_i ← R_i
        unique_i ← false
    end for
    for j = 1 to N do
        for all i ∈ S(r) do
            Send (R_i, r) to the right neighbor
        end for
        for each process p do
            Receive message (m, r) from its left neighbor
            if R_p > m then
                Do nothing
```

```
        else if R_p < m then
            R_p ← m
        else if R_p = m and R_p = uid_p and j = N then
            unique_p ← true
        end if
    end for
  end for
  for all p ∈ S(r) do
    if unique_p = true then
        p declares itself as leader
        End While loop
    else if unique_p = false and R_p = uid_p then
        Add p to S(r + 1)
    end if
  end for
  r ← r + 1
end while
```

2 Reconsider Exercise 1 (20 points)

I believe that it cannot be done. Impossibility proof should run along the following lines suggested by Toma Pirtskelani.

- assume a randomized algorithm selects a leader L after r steps on ring size N.
- rerun the algorithm on a ring of size $2N$. For every random choice R_i^t of a node i in any step t of the small ring make the same random choice $R_i^t = R_{i+N \bmod 2N}^t$ for nodes i and $i + N \bmod 2N$. OK, that's highly unlikely but not impossible.
- prove by induction for the states s_i^t of process i before step t

$$s_i^t = s_{i+N \bmod 2N}^t$$

- in this run L and $L + N \bmod 2N$ will declare themselves leaders after r steps.

3 One's complement numbers (20Pt)

Let $a \in \mathbb{B}^n$, then

$$[[a]] = \begin{cases} \langle a_{tl} \rangle & a_{n-1} = 0 \\ \langle a_{tl} \rangle - 2^{(n-1)} + 1 & a_{n-1} = 1 \end{cases}$$

$-[[a]] = [[\bar{a}]]$

$$\begin{aligned}
[[\bar{a}]] + [[a]] &= \langle \overline{a_{tl}} \rangle - \overline{a_{n-1}} * (2^{n-1} - 1) + \langle a_{tl} \rangle - a_{n-1} * (2^{n-1} - 1) \\
&= \langle \overline{a_{tl}} \rangle - \overline{a_{n-1}} * 2^{n-1} + \overline{a_{n-1}} + \langle a_{tl} \rangle - a_{n-1} * 2^{n-1} + a_{n-1} \\
&= \langle \overline{a_{tl}} \rangle - \overline{a_{n-1}} * 2^{n-1} + \langle a_{tl} \rangle - a_{n-1} * 2^{n-1} + 1 \\
&= -2^{n-1} + \langle \overline{a_{tl}} \rangle + \langle a_{tl} \rangle + 1 \\
&= -2^{n-1} + \sum_{i=0}^{n-2} a_i \cdot 2^i + \sum_{i=0}^{n-2} \overline{a_i} \cdot 2^i + 1 \\
&= -2^{n-1} + \sum_{i=0}^{n-2} 2^i + 1 \\
&= -2^{n-1} + 2^{n-1} - 1 + 1 \\
&= 0
\end{aligned}$$

$[[a]] \leq 0 \leftrightarrow a_{n-1} = 1 \vee a = 0^n$

Proof:
By definition, if $[[a]] \leq 0$, then:

$$a_{n-1} = 0 \wedge \langle a_{\mathrm{tl}} \rangle \leq 0 \vee a_{n-1} = 1 \wedge (\langle a_{\mathrm{tl}} \rangle - 2^{(n-1)} + 1) \leq 0$$

We know that $\langle a_{\mathrm{tl}} \rangle \geq 0$ and $\langle a_{\mathrm{tl}} \rangle = 0$ when $a = 0^n$. Thus, we have:

$$a_{n-1} = 0 \wedge a = 0^n \vee a_{n-1} = 1 \wedge (\langle a_{\mathrm{tl}} \rangle - 2^{(n-1)} + 1) \leq 0$$

Since $(\langle a_{\mathrm{tl}} \rangle - 2^{(n-1)} + 1) \leq 0$ is always true, we obtain:

$$a_{n-1} = 0 \wedge a = 0^n \vee a_{n-1} = 1$$

$$a = 0^n \vee a_{n-1} = 1$$

This completes the proof.

4 Correctness of Polynomial Division (20 Pt)

$f_{i+1} = f - q_i g$ for all i

Proof by induction:

base case: $i = 0$

$$\text{definition } f_{i+1} = f_i - gt_i$$
$$\text{from definition we know } q_0 = t_0 \text{ and } f_0 = f$$
$$f_1 = f - q_0 g$$

case: for n holds and prove for n+1

$$\begin{aligned}
f_{n+1} &= f_n - t_n g && \text{definition} \\
&= f - q_{n-1} g - t_n g && \text{induction hypothesis} \\
&= f - (q_{n-1} + t_n) g \\
&= f - q_n g && \text{definition } q_i = q_{i-1} + t_i
\end{aligned}$$

$a_{i,n-i} \neq 0 \rightarrow \deg(f_{i+1}) < \deg(f_i)$

Proof by induction:

base case: $i = 0$

$$f_0 = f = \sum_{j=0}^{n} a_{0,j} x^j$$

$$\begin{aligned}
f_1 &= f_0 - gt_0 \\
&= \sum_{j=0}^{n} a_{0,j} x^j - \frac{a_{0,n}}{b_m} \sum_{j=0}^{m} b_j x^{j+n-m} \\
&= \sum_{j=0}^{n} a_{0,j} x^j - \frac{a_{0,n}}{b_m} \sum_{j=0}^{m-1} b_j x^{j+n-m} - \frac{a_{0,n}}{b_m} * b_m x^{m+n-m} \\
&= \sum_{j=0}^{n} a_{0,j} x^j - \frac{a_{0,n}}{b_m} \sum_{j=0}^{m-1} b_j x^{j+n-m} - a_{0,n} x^n \\
&= \sum_{j=0}^{n-1} a_{0,j} x^j - \frac{a_{0,n}}{b_m} \sum_{j=0}^{m-1} b_j x^{j+n-m}
\end{aligned}$$

In both sums we have left maximum power x^{n-1}.

for k holds and prove for k+1:

$$\begin{aligned}
f_{k+1} &= f_k - gt_k \\
&= \sum_{j=0}^{n} a_{k,j} x^j - \frac{a_{k,n-k}}{b_m} \sum_{j=0}^{m} b_j x^{j+n-m-k} \\
&= \sum_{j=0}^{n} a_{k,j} x^j - \frac{a_{k,n-k}}{b_m} \sum_{j=0}^{m-1} b_j x^{j+n-m-k} - a_{k,n-k} x^{n-k}
\end{aligned}$$

By induction hypothesis we know that from 0 to k $deg(f_{i+1}) < deg(f_i)$ so in each step we should reduce polynomial at least by one degree

$$\begin{aligned} &\leq \sum_{j=0}^{n-k} a_{k,j}x^j - \frac{a_{k,n-k}}{b_m}\sum_{j=0}^{m-1} b_j x^{j+n-m-k} - a_{k,n-k}x^{n-k} \\ &= \sum_{j=0}^{n-k-1} a_{k,j}x^j - \frac{a_{k,n-k}}{b_m}\sum_{j=0}^{m-1} b_j x^{j+n-m-k} \end{aligned}$$

In both sums we have left maximum power x^{n-k-1}.

5 CRC (20 Pt)

We have message polynomial

$$u(x) = x^8 + x^5 + x$$

It has degree 8 and hence 9 koefficients, thus the message length is $k = 9$. The divisor polynomial

$$g(x) = x^4 + x + 1$$

has degree $n - k = 4$. This gives a message length

$$n = k + (n - k) = 13$$

3 Polynomial division of

$$u(x) \cdot x^{n-k} = x^{12} + x^9 + x^5$$

by $g(x)$ gives quotient

$$a(x) = x^8 + x^4 + 1$$

and remainder

$$s(x) = x + 1$$

Let's better check this:

$$\begin{aligned} a(x)g(x) = &\left(x^8 + x^4 + 1\right)\left(x^4 + x + 1\right) \\ =&x^{12} + x^8 + x^4 \\ &+ x^9 + x^5 + x \\ &+ x^8 + x^4 + 1 \\ =&x^{12} + x^9 + x^5 + x + 1 \\ =&u(x) \cdot x^{n-k} + s(x) \end{aligned}$$

You better check this! Thus

$$u(x) \cdot x^{n-k} + s(x) = x^{12} + x^9 + x^5 + x + 1$$

and the message sent is 1001000100011